FO-5-517AU
OA ref iV
4

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, G06K 9/00 — A1

(11) International Publication Number: WO 99/26372

(43) International Publication Date: 27 May 1999 (27.05.99)

(21) International Application Number: PCT/US98/23327

(22) International Filing Date: 2 November 1998 (02.11.98)

(30) Priority Data:
08/970,304 14 November 1997 (14.11.97) US

(71) Applicant *(for all designated States except US)*: DIGITAL PERSONA, INC. [US/US]; Suite 226, 805 Veterans Boulevard, Redwood City, CA 94063 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BJORN, Vance [US/US]; 431 Clifton Avenue, San Carlos, CA 94070 (US).

(74) Agents: SALTER, James, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

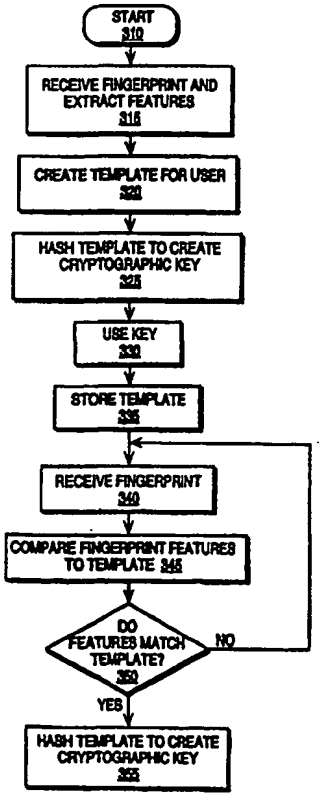
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CRYPTOGRAPHIC KEY GENERATION USING BIOMETRIC DATA

(57) Abstract

A method and apparatus for generating a cryptographic key using biometric data is provided. A fingerprint is received, and features are extracted from the fingerprint (315). Theses features may include one or more of the following: a message is created based on the features of the fingerprint. For one embodiment, the message is a template including the features (320). For another embodiment, the message is a subset of features not included in a template. A message digest function is applied to the message to create a cryptographic key (355). Another embodiment of the present invention uses features of the fingerprint image to generate a digital certificate. The public key used for the digital certificate is based on a fingerprint image.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

CRYPTOGRAPHIC KEY GENERATION USING BIOMETRIC DATA

FIELD OF THE INVENTION

The present invention relates to cryptography, and more specifically, to the generation of a unique cryptographic key using biometric data.

BACKGROUND

As more and more information is moving into electronic form, encryption is becoming more common. One prior art method of encryption is public key encryption, an encryption scheme in which each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using the recipient's private key. Messages are signed using the sender's public key and can only be decrypted using the sender's public key. The need for sender and receiver to share secret information (keys) via some secure channel is eliminated-- all communications involve only public keys, and no private key needs to be transmitted or shared. Public-key cryptography can be used for authentication (digital signatures) as well as for privacy (encryption). Other encryption schemes, such as symmetric key encryption rely on an exchange of keys.

However, keys generally are 64 bit numbers or larger and users do not memorize their keys. Rather, users store their key on their computer system. Because computer systems are rarely truly secure, the key may be taken from a computer system. In order to prevent this, the key may be stored in a password protected file. However, passwords may be broken.

Additionally, the system is only as secure as the least secure level. Therefore, what is needed is a secure cryptographic key that is easily usable by the user, but not accessible to third parties.

SUMMARY OF THE INVENTION

The present invention relates to cryptography, and more specifically, to the generation of a unique cryptographic key using biometric data. A fingerprint is received, and features are extracted from the fingerprint. These features may include one or more of the following: A message is created based on the features of the fingerprint. For one embodiment, the message is a template including the features. For another embodiment, the message is a subset of features not included in a template. For another embodiment, the message is ghost points not corresponding to the features in the template. A message digest function is applied to the message to create a cryptographic key.

Another embodiment of the present invention uses features of the fingerprint image to generate a digital certificate. The public key used for the digital certificate is based on a fingerprint image. In one embodiment, the digital certificate contains a template including the fingerprint image or the features extracted from the fingerprint image. Verification of this template provides additional security to the validity of the digital certificate.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Figure 1 is a computer system on which the present invention may be implemented.

Figure 2 is a block diagram of one embodiment of the apparatus of the present invention.

Figure 3 is a flowchart illustrating one embodiment of generating and using the cryptographic key of the present invention.

Figure 4 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention.

Figure 5 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention.

Figure 6 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention.

Figure 7 is a flowchart illustrating one embodiment of the generating and using a digital certificate according to the present invention.

Figure 8 is a flowchart illustrating another embodiment of the generating and using a digital certificate according to the present invention.

Figure 9 is an illustration of one example of a fingerprint including marked minutiae and ghost points.

DETAILED DESCRIPTION

A method and apparatus for generating a cryptographic key using biometric data is described. In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form in order to avoid unnecessarily obscuring the present invention.

Figure 1 is a computer system on which the present invention may be implemented. Figure 1 is a diagram of one embodiment of the digital

system on which the present invention may be implemented. Digital system 10 comprises a system bus 110 or other communication means for communicating information, and a processor 120 coupled with system bus 110 for processing information. Digital system 100 also comprises a read only memory (ROM) and/or other static storage device 135 coupled to system bus 110 for storing static information and instructions for processor 120. The digital system 100 further comprises a main memory 130, a dynamic storage device for storing information and instructions to be executed. Main memory 130 also may be used for storing temporary variables or other intermediate information during execution of instructions. In one embodiment the main memory 130 is dynamic random access memory (DRAM).

Digital system 100 can also be coupled via system bus 110 to a display device 150, such as a cathode ray tube (CRT) or liquid crystal display (LCD) screen, for displaying information to a user. An alphanumeric input device 155 is typically coupled to system bus 110 for communicating information and command selections to processor 120. Another type of user input device is cursor control device 160, such as a mouse, a trackball, trackpad, or cursor direction keys for communicating direction information and command selections to processor 120 and for controlling cursor movement on display device 150. Alternatively, other input devices such as a stylus or pen can be used to interact with the display. The digital system 100 may further be coupled via the system bus 110 to a network communication device 165. The network communication device 165 may be utilized to couple the digital system to other digital systems, servers, and networks.

Digital system 100 further comprises a universal serial bus (USB) controller 180, a bus controller for controlling a universal serial bus (USB)

185. The USB 185 is for coupling USB devices 190 to the digital system 100. A fingerprint sensor 195 is coupled to the digital system 100 via the USB 185. Alternately, the fingerprint sensor 195 may be coupled to the digital system 100 via the network communication device 165.

Figure 2 is a block diagram of the apparatus of the present invention. For one embodiment, the cryptographic key generation unit 210 includes a database 220. The database 220 stores templates of fingerprints. For one embodiment, no database 220 is used, and templates are either not used or are stored with the encrypted files.

A temporary storage unit 230 stores data used for the processing and generation of the cryptographic key. For one embodiment, the temporary storage unit 230 is emptied once matching/generation is completed. For one embodiment, the cryptographic key generated is only stored in the temporary storage unit 230 for sufficient time to use it, and is then erased.

A feature extraction unit 240 receives a fingerprint from the fingerprint sensor 195. The feature extraction unit 240 extracts relevant features from the fingerprint. An additional feature extraction unit 245 extracts other features than minutiae. For one embodiment, these features may include minutiae, including location and orientation; spatial frequency; curvature; ridge count; ridge distance/curvature between points; relation to global features; code words generated by vector quantization to encode subunit spatial characteristics; etc. These features are stored in the temporary storage unit 230.

For one embodiment, the matching unit 250 is included in the cryptographic key generation unit 210. The matching unit 250 compares the extracted features of the fingerprint and the template and determines whether the fingerprint matches a template. For one embodiment, if the user is not known, the template creation unit 260 creates a template of the new user, and adds it to the database 220.

The hashing unit 280 creates a hash of the message created by the message creation unit 270. For one embodiment, a one-way hash function or message digest function is used to create the hash. The one-way hash function takes a variable-length message and produces a fixed-length hash. Given the hash it is computationally impossible to find a message with that hash; in fact one can not determine any usable information about a message with that hash. For some one-way hash functions it's also computationally impossible to determine two messages which produce the same hash. For one embodiment, this fixed-length hash is the cryptographic key associated with the user's fingerprint. For another embodiment, this fixed-length hash is the basis used to generate the cryptographic key. For one embodiment, the one-way hash function used is MD5. Alternatively, other hash functions may be used. For one embodiment, the fixed-length is 128 bits.

For one embodiment, the ghost generation unit 290 is further included in the cryptographic key generation unit 210. The ghost point generation unit 290 is used to generate ghost points to be included in the template. The function of the ghost units is explained below.

The subtraction 270 may be included in the cryptographic key generation unit 210. The subtraction unit 270 is used to remove extracted fingerprint features from a template which includes both fingerprint features and ghost points, in order to obtain the ghost points.

Figure 3 is a flowchart illustrating one embodiment of generating and using the cryptographic key of the present invention. At block 310, the process starts. At block 315, a fingerprint is received from the user. The fingerprint may be encrypted or otherwise protected. For one embodiment, a time and date stamp is included in the encrypted fingerprint to assure that the fingerprint was not generated previously and resent. If the fingerprint is encrypted or otherwise protected, it is decrypted, and a digital fingerprint image is generated. The

features of the fingerprint are then extracted. These features may include one or more of the following: minutiae, including location and orientation; spatial frequency; curvature; ridge count; ridge distance/curvature between points; relation to global features; code words generated by vector quantization to encode subunit spatial characteristics; etc. Methods of extracting these features are known in the art.

At block 320, a template is created for the user. A template includes at least some of the features extracted from the fingerprint. For one embodiment, the template includes all of the identifying features extracted from the print.

At block 325, the template is hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, known techniques are used on the hash to generate the cryptographic key. This cryptographic key is identified with the specific fingerprint, and thus with a specific user. For one embodiment, for a public key encryption, a private key is generated based on the hash. A public key is generated to correspond to the cryptographic key. Methods of generating a public key which corresponds to a private key are known in the art. Public key/private key pairs are known in the art, and are used to authenticate documents, encrypt documents, etc.

At block 330, the cryptographic key is used. For one embodiment, the cryptographic key is generated in order to do something specific. For example, the key may be used to sign a document with the user's private key. This allows the document to be decrypted with the user's public key, thus identifying the document as originating with the user. Alternately, a document may be encrypted with the user's public key, allowing decryption only with the user's private key, thus protecting the document from unauthorized users.

At block 335, the template is stored. The cryptographic key itself is not stored anywhere on the system. For one embodiment, the template is stored with the file for which it was used. Thus, if a document was encrypted, the

template is attached to the document itself. For another embodiment, the template is stored in a database, or other more centralized location.

The initial use of the key is now complete. A file may have been encrypted. Such a file may be stored on the system, sent, or otherwise disposed of by the user. If the user wishes to decrypt an encrypted document, or otherwise use the cryptographic key again, the flowchart is entered at block 340.

At block 340, the fingerprint is received from the user. As described again, various verification techniques may be used to make sure that the fingerprint is a genuine fingerprint. The features of the fingerprint are extracted.

At block 345, the fingerprint features, newly extracted, are compared to the template. As described above with respect to block 320, the template includes some or all of the features previously extracted from the fingerprint. The comparison tests whether the fingerprint received belongs to the same user as the template.

At block 350, the process tests whether the features match the template. This comparison may be done using any method known in the art. The comparison of a fingerprint and a template is known in the art. If the features do not match the template, the process continues to block 340. For one embodiment, a new fingerprint is requested. If the features do match, the process continues to block 355.

At block 355, the template is again hashed to create a cryptographic key. Since the template was used to generate the first cryptographic key, the same key is generated. The key can then be used in the above described manner.

Figure 4 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention.

At block 410, the process starts. At block 415, a fingerprint is received from the user. The fingerprint may be encrypted or otherwise protected. For one embodiment, a time and date stamp is included in the encrypted fingerprint

to assure that the fingerprint was not generated previously and resent. If the fingerprint is encrypted or otherwise protected, it is decrypted, and a digital fingerprint image is generated. The features of the fingerprint are then extracted. These features may include one or more of the following: minutiae, including location and orientation; spatial frequency; curvature; ridge count; ridge distance/curvature between points; relation to global features; etc. Methods of extracting these features are known in the art.

At block 420, a template is created for the user. A template includes at least some of the features extracted from the fingerprint. For one embodiment, the template includes only the minutiae location and orientations. Thus, may other features, such as spatial frequency, curvature, ridge count, ridge distance/curvature between points, relation to global features are not included in the template, and code words generated by vector quantization to encode subunit spatial characteristics; .

At block 425, these additional features are determined and placed into a temporary message.

At block 430, the message containing only the additional features are hashed. For one embodiment, this hash is the cryptographic key. For another embodiment, the hash is used to generate a cryptographic key. For one embodiment, the hash generates a private key. A corresponding public key is generated as well.

At block 435, the key is used, as described above.

At block 440, the template is stored. The template contains only the minutiae of the fingerprint. Therefore, even if a hacker accesses the template, the hacker can not deduce the cryptographic key. The additional features used to generate the cryptographic key are not included in the template.

The initial use of the key is complete at this point. The template may have been stored with the file(s) for which it was used. Alternately, the template may

be in a database. If the user wishes to reuse the key, to access the previously encrypted file, or to encrypt a new file, the process starts at block 450.

At block 450, the fingerprint is received from the user. As described above, various verification techniques may be used to make sure that the fingerprint is a genuine fingerprint. The features of the fingerprint are extracted.

At block 455, the fingerprint features, newly extracted, are compared to the template. As described above with respect to block 420, the template includes some of the features previously extracted from the fingerprint. The comparison tests whether the fingerprint received belongs to the same user as the template.

At block 460, the process tests whether the features match the template. This comparison may be done using any method known in the art. The comparison of a fingerprint and a template is known in the art. If the features do not match the template, the process continues to block 450. For one embodiment, a new fingerprint is requested. If the features do match, the process continues to block 465.

At block 465, additional features of the fingerprint are extracted.

At block 470, these additional features are determined and placed into a temporary message. The message containing only the additional features are then hashed to generate a cryptographic key. For one embodiment, the hash is used to generate a private key. A corresponding public key is generated as well. Because the additional features correspond to the same fingerprint, the message generated is identical to the original message. This results in reproducing the original cryptographic key. The key can now be used, as is known in the art.

Figure 5 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention. At block 510, the process starts.

At block 515, the fingerprint is received, and the features of the fingerprint are extracted. The features are those described above.

At block 520, ghost points are generated. The ghost points are false features which are placed into the fingerprint. Figure 9 illustrates a fingerprint with a plurality of marked minutiae 920. Figure 9 also includes ghost points 930 placed in clear areas 940 of the fingerprint. Clear areas 940 are areas which do not have actual, or probable, minutia points. For example, a clear area may be along a continuous ridge. Since minutia points are ridge beginnings, endings, or forks, along a continuous ridge, no minutia points are likely to occur. By selecting clear areas, areas 940 in which it is unlikely that there could be a minutia, errors are minimized. Ghost points 930 are assigned an orientation, in addition to the location. For alternative embodiment, ghost points 930 are not located in clear areas 940 but have orientations which are highly unlikely. Ridges in fingerprints are continuous, therefore, a ghost point along a ridge which points at a ninety degree angle from the direction of the ridge is highly unlikely. Alternative means of placing points that can be distinguished from real minutiae on comparison with the fingerprint may be used.

Returning to Figure 5, at block 525, a template is created including ghost points. The ghost points are included in the template without any notation. On examining the template, one can not differentiate between actual minutiae and ghost points. The way to identify ghost points is by examining the actual fingerprint.

At block 530, the extracted features are subtracted from the template. This leaves the ghost points which were added to the template. The ghost points are hashed, to create the cryptographic key.

At block 535, the cryptographic key may be used for any known uses. At block 540, the template, including the ghost points, are stored. For one embodiment, the template is stored with the files that were

encrypted/authenticated. For another embodiment, the template is stored in a database.

At block 540, the template, including the ghost points, is stored. The template may be stored in a database, or with the file(s) that were encrypted. At this point the cryptographic key has been used. In order to decrypt an encrypted file, or to use the key again, the process continues at block 550.

At block 550, the fingerprint is received, and the features are extracted.

At block 555, the features extracted from the fingerprint are compared to the template. For one embodiment, in examining the points of the template, comparing them to the fingerprint each of the points is examined separately.

At block 560, it is determined whether the features match the template. If the extracted features do not match, i.e. it is not the same user, the process returns to block 550. For one embodiment, a new fingerprint is automatically requested. If the extracted features do match, the process continues at block 565.

At block 565, the extracted features are subtracted from the template, leaving only the ghost points.

At block 570, the result, i.e. the ghost points, are hashed to create the cryptographic key. Because the cryptographic key is generated from the same set of ghost points as above in block 530, the same key is generated. Therefore, any files encrypted with the key may be decrypted.

Figure 6 is a flowchart illustrating another embodiment of generating and using the cryptographic key of the present invention. At block 610, the process starts.

At block 620, the fingerprint is received.

At block 630, the features of the fingerprint are extracted. The features may include minutiae, including location and orientation; spatial frequency; curvature; ridge count; ridge distance/curvature between points; relation to global features; code words generated by vector quantization to encode subunit

spatial characteristics; etc. These features may be further evaluated for clarity. For one embodiment, only those features with high clarity are retained.

At block 640, the features are hashed. This hash may be the cryptographic key. Alternatively, known algorithms may be used to generate a cryptographic key from the hash. The cryptographic key includes some or all of the features of the original fingerprint.

At block 650, the key may be used, to encrypt or authenticate files, or for any other purpose. The initial generation of the key is now complete. After the key is used, it is not retained. No template is generated.

In order to decrypt the file, or otherwise use the key again, the process is restarted at block 660. At block 660, the fingerprint is received.

At block 670, the features of the fingerprint are extracted. For one embodiment, these features are the same as the features extracted above, at block 630. For another embodiment, some additional features may be extracted. For one embodiment, the user may place his or her finger on the scanner multiple times, to generate a composite image which better represents the actual fingerprint image.

At block 680, the extracted features are hashed. This hash may be the cryptographic key. Alternatively, known algorithms may be used to generate a cryptographic key from the hash. This cryptographic key is identical to the cryptographic key generated at block 640. For one embodiment, the cryptographic key generated is a private key, and it and the corresponding public key, can be used to decrypt the previously encrypted file, or for other uses.

For one embodiment, generating the identical cryptographic key is a two step process. After the features are extracted, they may be jiggled slightly, to generate different hashes. That is, the features may be moved incrementally, to compensate for a user not placing his or her finger in exactly the same location as

when generating the original cryptographic key. For one embodiment, the initial features extracted are an initial condition for the cryptographic key. The hash generated from the initial features is used to search the local key space. Alternative methods of matching the positioning of the fingerprint may be used.

Figure 7 is a flowchart illustrating one embodiment of the generating and using a digital certificate according to the present invention. Digital certificates bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. The digital certificate makes it possible to verify a user's claim that they have the right to use a given key, helping to prevent the use of false keys to impersonate a user. Digital certificates are generally issued by a certification authority, and signed by the certification authority's private key. The certification authority certifies that the holder of the key pair is actually who he or she claims to be. The digital certificate generally includes the owner's public key, the owner's name, the expiration date of the public key, the name of the issuer (the certification authority), the serial number of the digital certificate, and the digital signature of the issuer. By sending the digital certificate, a user can make sure that an "authentic" copy of the public key of the user is known.

At block 710, the process starts. The registration process for obtaining the digital certificate is illustrated in blocks 715-730. The process for using the digital certificate is illustrated in blocks 735-770.

At block 715, the user sends a fingerprint template to the certification authority (CA) to include in a digital certificate. For one embodiment, the fingerprint template is a digital image of the fingerprint. For another embodiment, the fingerprint template is a template of features extracted from the fingerprint. The CA uses other information of the user's to verify the identity of the user. For example, a social security number may be used. Alternately, other similar information may be used to check the identity of the user whose fingerprint is received by the CA.

At block 720, a digital certificate is generated by the certification authority. In addition to including the above listed information in the certificate, the fingerprint template are also included by the certification authority. Thus, the owner of the fingerprint is further identified by the fingerprint template.

At block 725, the CA signs the digital key of the CA. The signature of the CA certifies that the digital certificate is authentic, to the best knowledge of the CA.

At block 730, the CA returns the digital certificate to the user. The user now has possession of the digital certificate, and can use it to authenticate his or her identity to third parties.

At block 735, the user wishes to use the digital certificate to authenticate his or her identity to a third party, for example Person A. The user sends the digital certificate to Person A to authenticate his or her identity.

At block 740, Person A decrypts the certificate with the certifying authority's public key. This tells Person A that the digital certificate is authentic. Thus, Person A knows that the digital certificate has not been altered.

At block 745, Person A retrieves the public key and fingerprint template enclosed in the certificate. Both the public key and fingerprint template identify the user associated with the user.

At block 750, Person A receives a file encrypted with the user's private key from the user. Additionally, a fingerprint is received from the user. For one embodiment, after Person A decrypts the certificate with the CA's public key, Person A requests the encrypted file and fingerprint from the user. For another embodiment, the user automatically sends a fingerprint and encrypted file when sending the digital certificate to Person A.

At block 755, Person A tests whether the public key, retrieved from the digital certificate, decrypts the file encrypted with the user's private key. A file encrypted with a private key may be decrypted with the corresponding public

key. Therefore, this informs Person A that the user is in possession of the private key corresponding to the digital certificate. For one embodiment, this encrypted file is encrypted with the above described encryption mechanism using the fingerprint of the person. If the public key decrypts the file, the process continues to block 765. If the public key does not decrypt the file, the process continues to block 760. At block 760, the user is rejected.

At block 765, the fingerprint received from the user is compared to the fingerprint template retrieved from the digital certificate. For one embodiment, the comparison is of a template of extracted features. If the fingerprint does not match the template, the process returns to block 760, and the user is rejected. If the fingerprint matches the fingerprint template, the process continues to block 770, and the user is accepted. At this point Person A knows that the digital certificate is authentic, and is associated with the user who is currently using the certificate. This provides an additional level of security for using digital certificates.

Figure 8 is a flowchart illustrating another embodiment of the generating and using a digital certificate according to the present invention.

At block 810, the process starts. The registration process for obtaining the digital certificate is illustrated in blocks 815-825. The process for using the digital certificate is illustrated in blocks 830-860.

At block 815, the user sends a public key to the certification authority (CA) to be included in the digital certificate. The CA uses other information of the user's to verify the identity of the user. For example, a social security number may be used. Alternately, other similar information may be used to check the identity of the user.

At block 820, the CA generates the digital certificate including the public key, and signs it with the digital key of the CA. The signature of the CA certifies that the digital certificate is authentic, to the best knowledge of the CA.

At block 825, the CA returns the digital certificate to the user. The user now has possession of the digital certificate, and can use it to authenticate his or her identity to third parties.

At block 830, the user wishes to use the digital certificate to authenticate his or her identity to a third party, for example Person A. The user sends the digital certificate to Person A to authenticate his or her identity.

At block 835, Person A decrypts the certificate with the certifying authority's public key. This tells Person A that the digital certificate is authentic. Thus, Person A knows that the digital certificate has not been altered.

At block 840, Person A retrieves the public key enclosed in the certificate. Both the public key identifies the user associated with the user.

At block 845, Person A receives a file encrypted with the user's private key from the user. The private key used by the user is generated from the user's fingerprint, as described above.

For one embodiment, after Person A decrypts the certificate with the CA's public key, Person A requests the encrypted file from the user. For another embodiment, the user automatically sends an encrypted file when sending the digital certificate to Person A.

At block 850, Person A tests whether the public key, retrieved from the digital certificate, decrypts the file encrypted with the user's private key. A file encrypted with a private key may be decrypted with the corresponding public key. Therefore, this informs Person A that the user is in possession of the private key corresponding to the digital certificate. For one embodiment, this encrypted file is encrypted with the above described encryption mechanism using the fingerprint of the person.

If the public key decrypts the file, the process continues to block 860, and the user is validated. If the public key does not decrypt the file, the process continues to block 855, and the user is rejected.

At block 765, the fingerprint received from the user is compared to the fingerprint template retrieved from the digital certificate. For one embodiment, the comparison is of a template of extracted features. If the fingerprint does not match the template, the process returns to block 760, and the user is rejected. If the fingerprint matches the fingerprint template, the process continues to block 770, and the user is accepted. At this point Person A knows that the digital certificate is authentic, and is associated with the user who is currently using the certificate. This provides an additional level of security for using digital certificates.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. The present invention should not be construed as limited by such embodiments and examples, but rather construed according to the following claims.

CLAIMS

What is claimed is:

1. A method comprising the computer implemented steps of:

receiving a fingerprint;

extracting features from the fingerprint;

creating a message based on the features of the fingerprint;

applying a message digest function to the message to create a cryptographic key.

2. The method of claim 1, wherein said step of creating the message comprises the step of creating a template including the features of the fingerprint, wherein said template comprises the message.

3. The method of claim 2, further comprising a step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

retrieving the template;

comparing the new fingerprint with the template;

if the new fingerprint matches the template, applying the message digest function to the template to generate the cryptographic key.

4. The method of claim 1, wherein said step of creating the message comprises the step of extracting additional features from the fingerprint, the additional features comprising the message.

5. The method of claim 4 further comprising the step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

retrieving the message;

extracting a primary set of features from the new fingerprint;

extracting a secondary set of features from the new fingerprint;

comparing the primary set of features to the message;

if the primary set of features match the message, applying the message digest function to the secondary set of features to create the cryptographic key.

6. The method of claim 1, wherein said step of creating the message comprises the steps of:

creating ghost points not corresponding to features of the fingerprint;

creating a template including the features and the ghost points;

subtracting the features from the template, leaving a ghost template, the ghost template being the message; and

storing the template.

7. The method of claim 6, further comprising the step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

retrieving the template;

extracting a new set of features from the new fingerprint;

comparing the new set of features to the template;

and if the new set of features match the template:

subtracting the new set of features from the template, generating the ghost template;

applying the message digest function to the ghost template to create the cryptographic key.

8. The method of claim 1, wherein said step of creating the message comprises the step of combining the features of the fingerprint to create the message.

9. The method of claim 8, further comprising a step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

extracting features from the new fingerprint;

creating a template of the features of the new fingerprint;

applying the message digest function to the template to create a new cryptographic key, the new cryptographic key identical to the cryptographic key previously generated.

10. A method comprising the computer implemented steps of:

receiving a fingerprint;

extracting features from the fingerprint;

creating a template of the features of the fingerprint;

applying a message digest function to the template to create a cryptographic key.

11. The method of claim 10, further comprising:

storing the template with each file that is encrypted using the cryptographic key.

12. The method of claim 10, further comprising:

storing the template in a database.

13. The method of claim 10, further comprising a step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

retrieving the template;

comparing the new fingerprint with the template;

if the new fingerprint matches the template, applying the message digest function to the template to generate the cryptographic key.

14. The method of claim 10, wherein said step of applying the message digest function comprises an MD5 algorithm.

15. The method of claim 10, wherein the template is not stored.

16. The method of claim 15, further comprising a step of retrieving the cryptographic key comprising the steps of:

receiving a new fingerprint;

extracting features from the new fingerprint;

creating a new template of the features of the new fingerprint;

applying the message digest function to the new template to create a new cryptographic key, the new cryptographic key identical to the cryptographic key previously generated.

17. A method comprising the computer implemented steps of:

receiving a fingerprint;

extracting a first set of features from the fingerprint;

extracting a second set of features from the fingerprint;

creating a template of the first set of features;

applying a message digest function to the second set of features to create a cryptographic key; and

storing the template with the first set of features.

18. The method of claim 17 further comprising the step of retrieving the cryptographic key including the steps of:

receiving a new fingerprint;

retrieving the template;

extracting a primary set of features from the new fingerprint;

extracting a secondary set of features from the new fingerprint;

comparing the primary set of features to the template;

if the primary set of features match the template, applying the message digest function to the secondary set of features to create the cryptographic key.

19. A method comprising the computer implemented steps of:

receiving a fingerprint;

extracting a set of features from the fingerprint;

generating ghost points, not corresponding to actual features of the fingerprint;

creating a template of the set of features and the ghost points;

subtracting the set of features from the template, generating a ghost template;

applying a message digest function to the ghost template to create a cryptographic key; and

storing the template.

20. The method of claim 19, further comprising the step of retrieving the cryptographic key including the steps of:

receiving a new fingerprint;

retrieving the template;

extracting a new set of features from the new fingerprint;

comparing the new set of features to the template;

and if the new set of features match the template:

subtracting the new set of features from the template, generating a new ghost template;

applying the message digest function to the new ghost template to create a new cryptographic key.

21. A method comprising the computer implemented steps of:

a certifying authority receiving a public key corresponding to a private key generated based on a user's fingerprint;

including the public key in a digital certificate;

signing the digital certificate with a private key of the certifying authority.

22. The method of claim 21, further comprising the steps of:

sending the digital certificate to a third party for authentication of the user;

the third party decrypting the digital certificate; and

the user sending a message encrypted with the user's fingerprint based private key; and

the third party decrypting the message with the public key included in the digital certificate to verify an identity of the user.

23. A method of claim 21, wherein said digital certificate further includes a fingerprint template.

24. The method of claim 23, further comprising the steps of:

sending the digital certificate to a third party for authentication of the user;

the third party decrypting the digital certificate; and

the user sending a fingerprint image to the third party; and

the third party comparing the fingerprint image to the fingerprint template to verify an identity of the user.

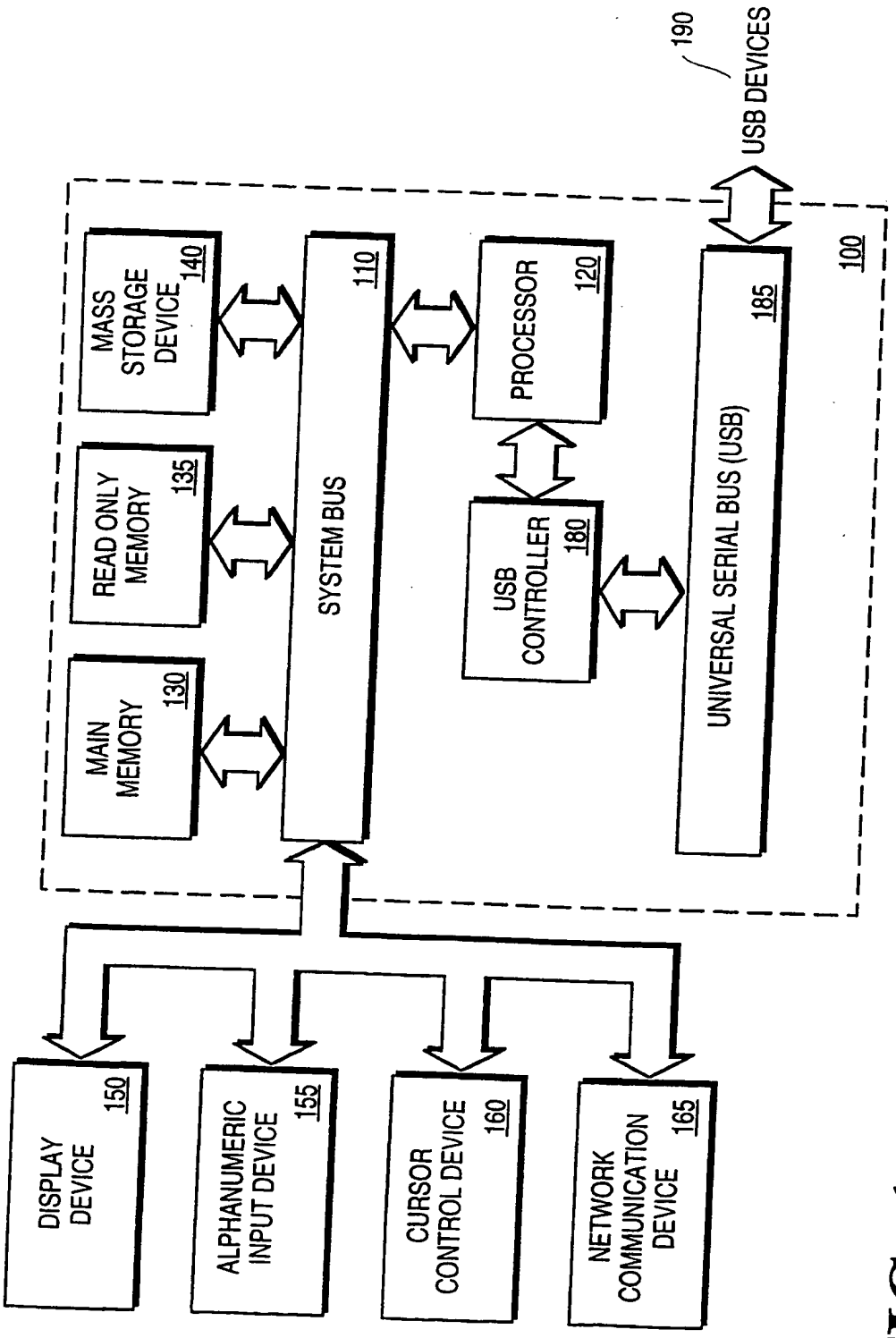

190
USB DEVICES
100
MASS STORAGE DEVICE 140
110
SYSTEM BUS
120
PROCESSOR
185
UNIVERSAL SERIAL BUS (USB)
READ ONLY MEMORY 135
USB CONTROLLER 180
MAIN MEMORY 130
DISPLAY DEVICE 150
ALPHANUMERIC INPUT DEVICE 155
CURSOR CONTROL DEVICE 160
NETWORK COMMUNICATION DEVICE 165

FIG. 1

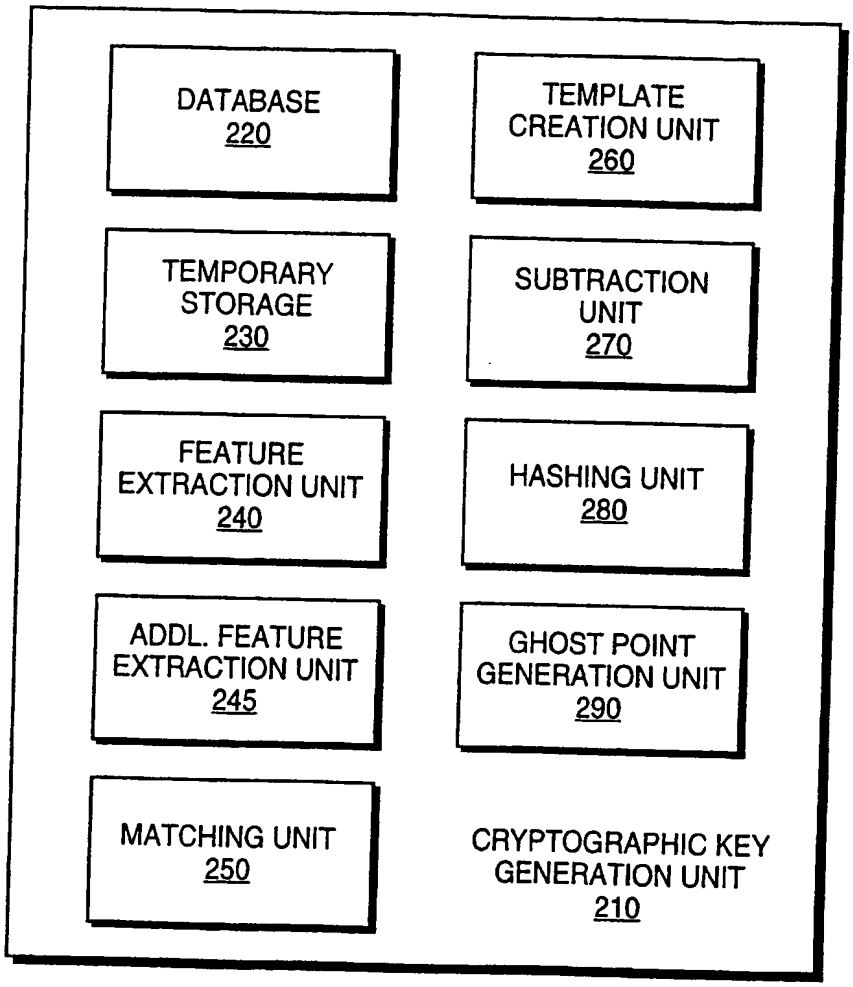

DATABASE
220
TEMPLATE
CREATION UNIT
260
TEMPORARY
STORAGE
230
SUBTRACTION
UNIT
270
FEATURE
EXTRACTION UNIT
240
HASHING UNIT
280
ADDL. FEATURE
EXTRACTION UNIT
245
GHOST POINT
GENERATION UNIT
290
MATCHING UNIT
250
CRYPTOGRAPHIC KEY
GENERATION UNIT
210

FIG. 2

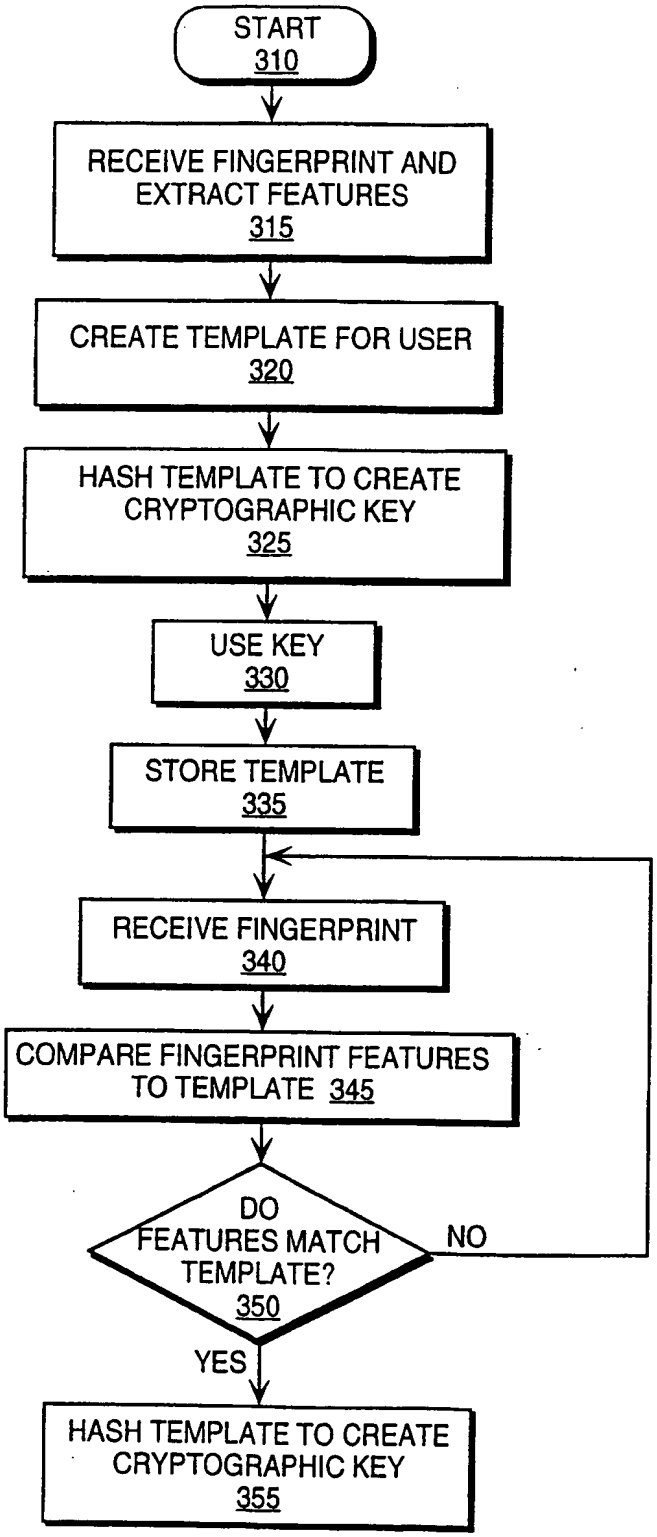

START
310
RECEIVE FINGERPRINT AND EXTRACT FEATURES
315
CREATE TEMPLATE FOR USER
320
HASH TEMPLATE TO CREATE CRYPTOGRAPHIC KEY
325
USE KEY
330
STORE TEMPLATE
335
RECEIVE FINGERPRINT
340
COMPARE FINGERPRINT FEATURES TO TEMPLATE 345
DO FEATURES MATCH TEMPLATE?
350
NO
YES
HASH TEMPLATE TO CREATE CRYPTOGRAPHIC KEY
355

FIG. 3

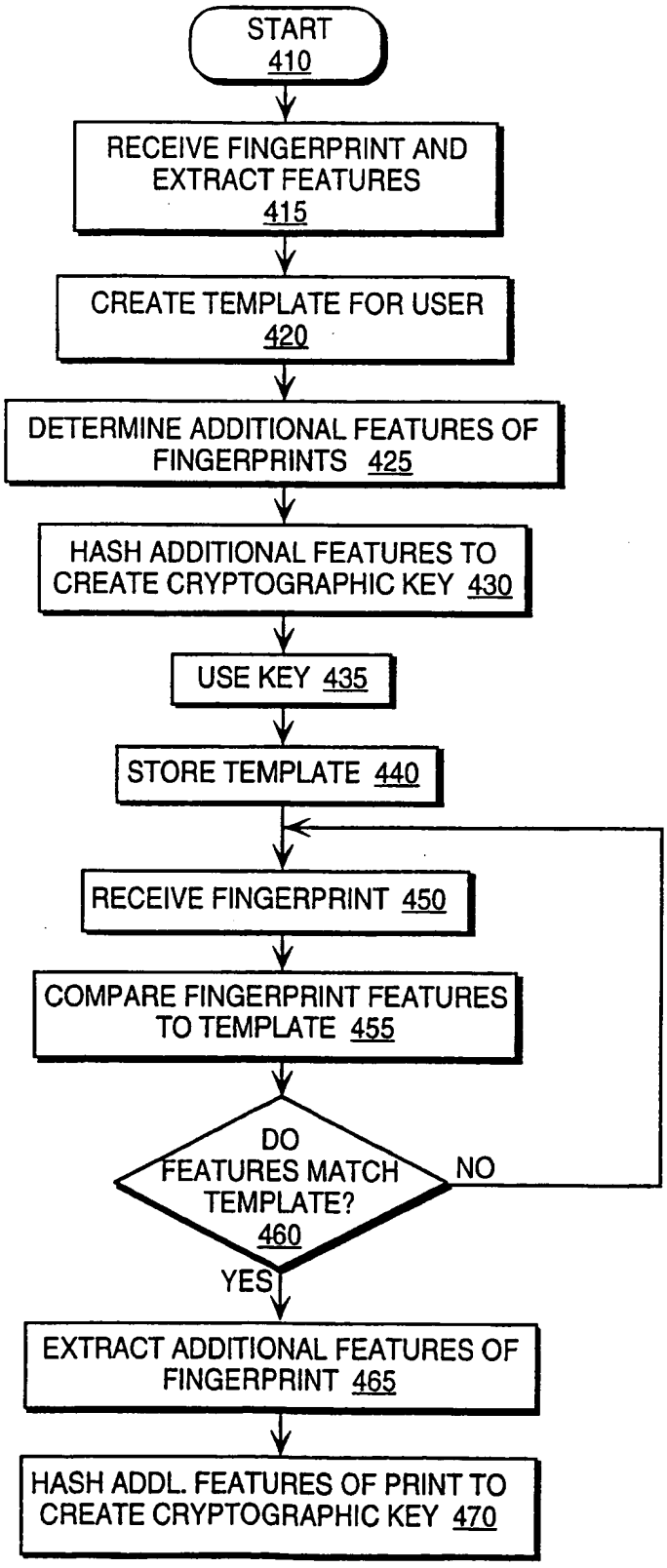

START
410
RECEIVE FINGERPRINT AND EXTRACT FEATURES
415
CREATE TEMPLATE FOR USER
420
DETERMINE ADDITIONAL FEATURES OF FINGERPRINTS 425
HASH ADDITIONAL FEATURES TO CREATE CRYPTOGRAPHIC KEY 430
USE KEY 435
STORE TEMPLATE 440
RECEIVE FINGERPRINT 450
COMPARE FINGERPRINT FEATURES TO TEMPLATE 455
DO FEATURES MATCH TEMPLATE?
460
NO
YES
EXTRACT ADDITIONAL FEATURES OF FINGERPRINT 465
HASH ADDL. FEATURES OF PRINT TO CREATE CRYPTOGRAPHIC KEY 470

FIG. 4

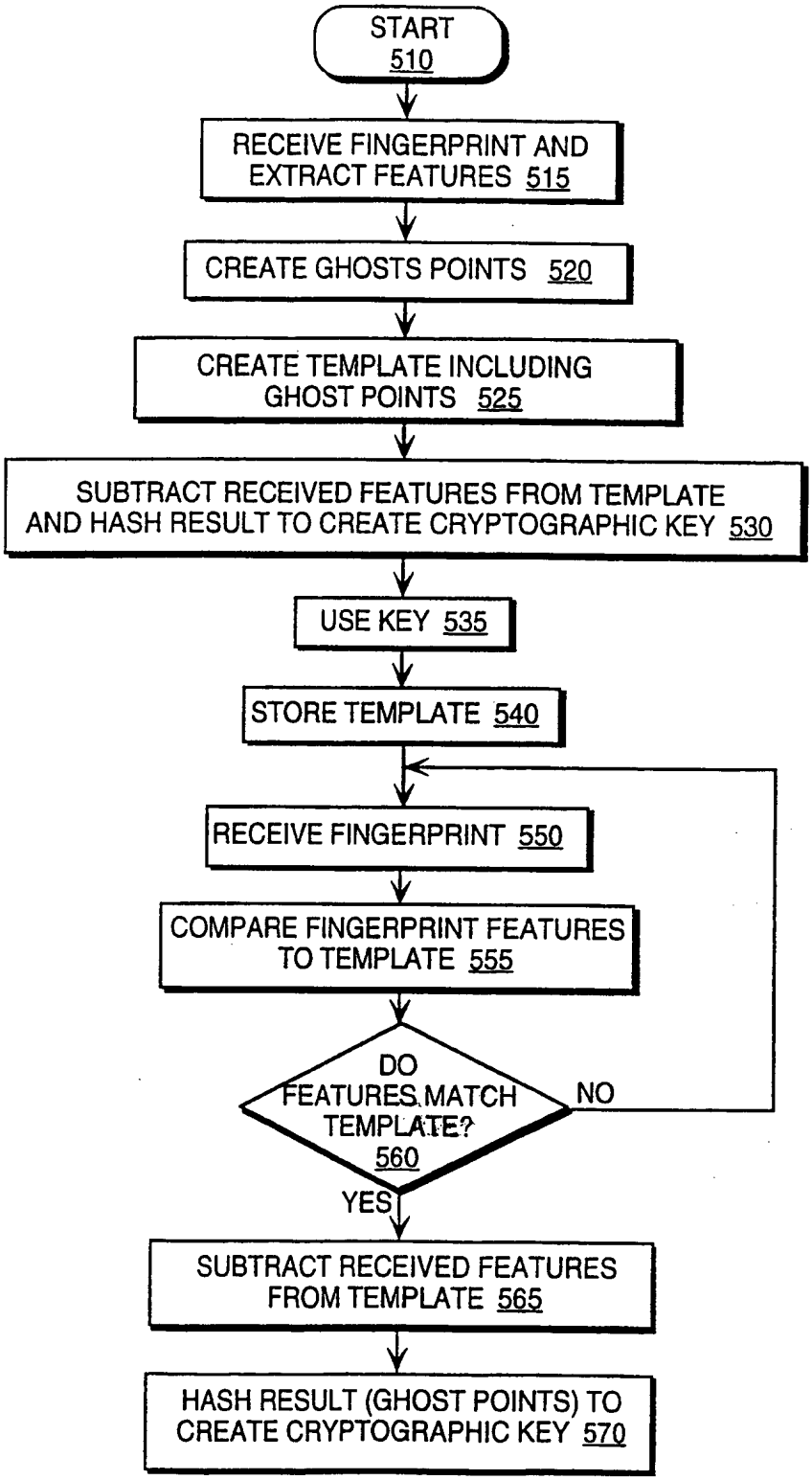

START 510
RECEIVE FINGERPRINT AND EXTRACT FEATURES 515
CREATE GHOSTS POINTS 520
CREATE TEMPLATE INCLUDING GHOST POINTS 525
SUBTRACT RECEIVED FEATURES FROM TEMPLATE AND HASH RESULT TO CREATE CRYPTOGRAPHIC KEY 530
USE KEY 535
STORE TEMPLATE 540
RECEIVE FINGERPRINT 550
COMPARE FINGERPRINT FEATURES TO TEMPLATE 555
DO FEATURES MATCH TEMPLATE? 560
NO
YES
SUBTRACT RECEIVED FEATURES FROM TEMPLATE 565
HASH RESULT (GHOST POINTS) TO CREATE CRYPTOGRAPHIC KEY 570

FIG. 5

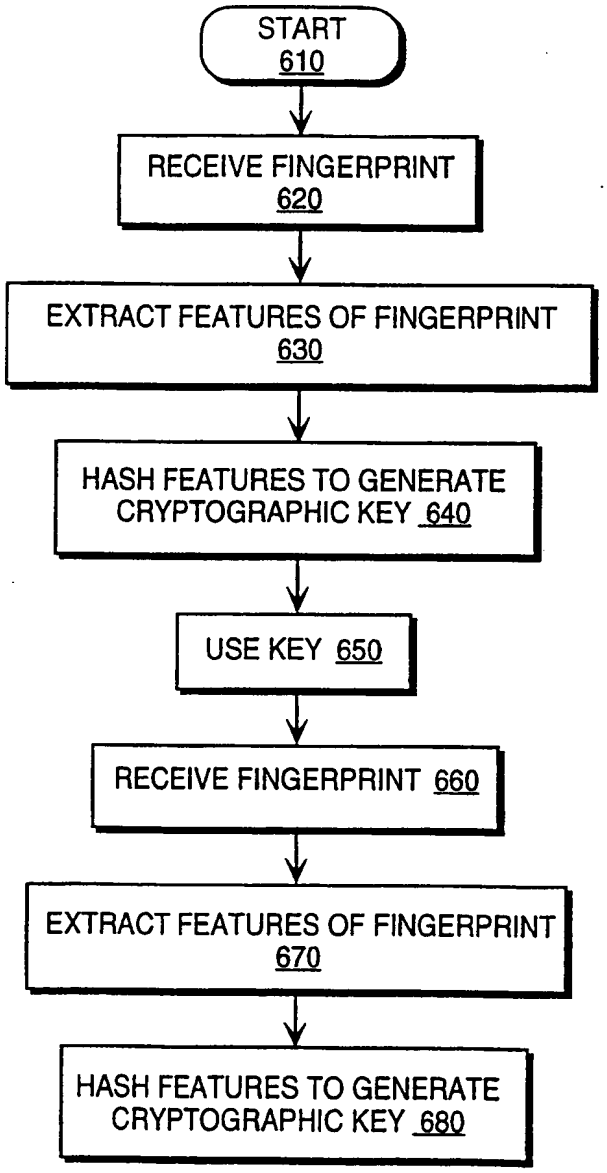

START
610
RECEIVE FINGERPRINT
620
EXTRACT FEATURES OF FINGERPRINT
630
HASH FEATURES TO GENERATE
CRYPTOGRAPHIC KEY 640
USE KEY 650
RECEIVE FINGERPRINT 660
EXTRACT FEATURES OF FINGERPRINT
670
HASH FEATURES TO GENERATE
CRYPTOGRAPHIC KEY 680

FIG. 6

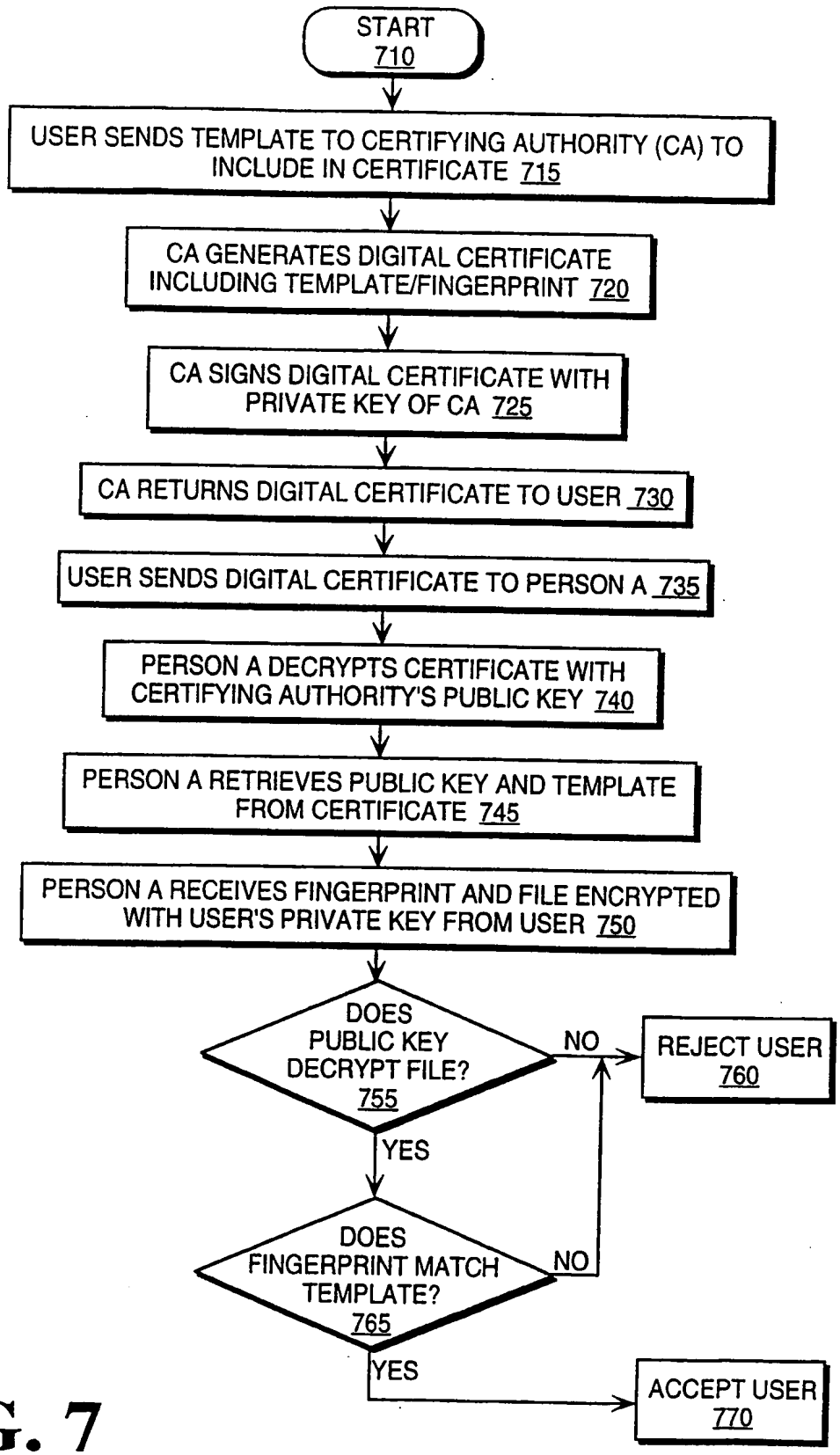

START
710
USER SENDS TEMPLATE TO CERTIFYING AUTHORITY (CA) TO INCLUDE IN CERTIFICATE 715
CA GENERATES DIGITAL CERTIFICATE INCLUDING TEMPLATE/FINGERPRINT 720
CA SIGNS DIGITAL CERTIFICATE WITH PRIVATE KEY OF CA 725
CA RETURNS DIGITAL CERTIFICATE TO USER 730
USER SENDS DIGITAL CERTIFICATE TO PERSON A 735
PERSON A DECRYPTS CERTIFICATE WITH CERTIFYING AUTHORITY'S PUBLIC KEY 740
PERSON A RETRIEVES PUBLIC KEY AND TEMPLATE FROM CERTIFICATE 745
PERSON A RECEIVES FINGERPRINT AND FILE ENCRYPTED WITH USER'S PRIVATE KEY FROM USER 750
DOES PUBLIC KEY DECRYPT FILE? 755
NO
REJECT USER 760
YES
DOES FINGERPRINT MATCH TEMPLATE? 765
NO
YES
ACCEPT USER 770

FIG. 7

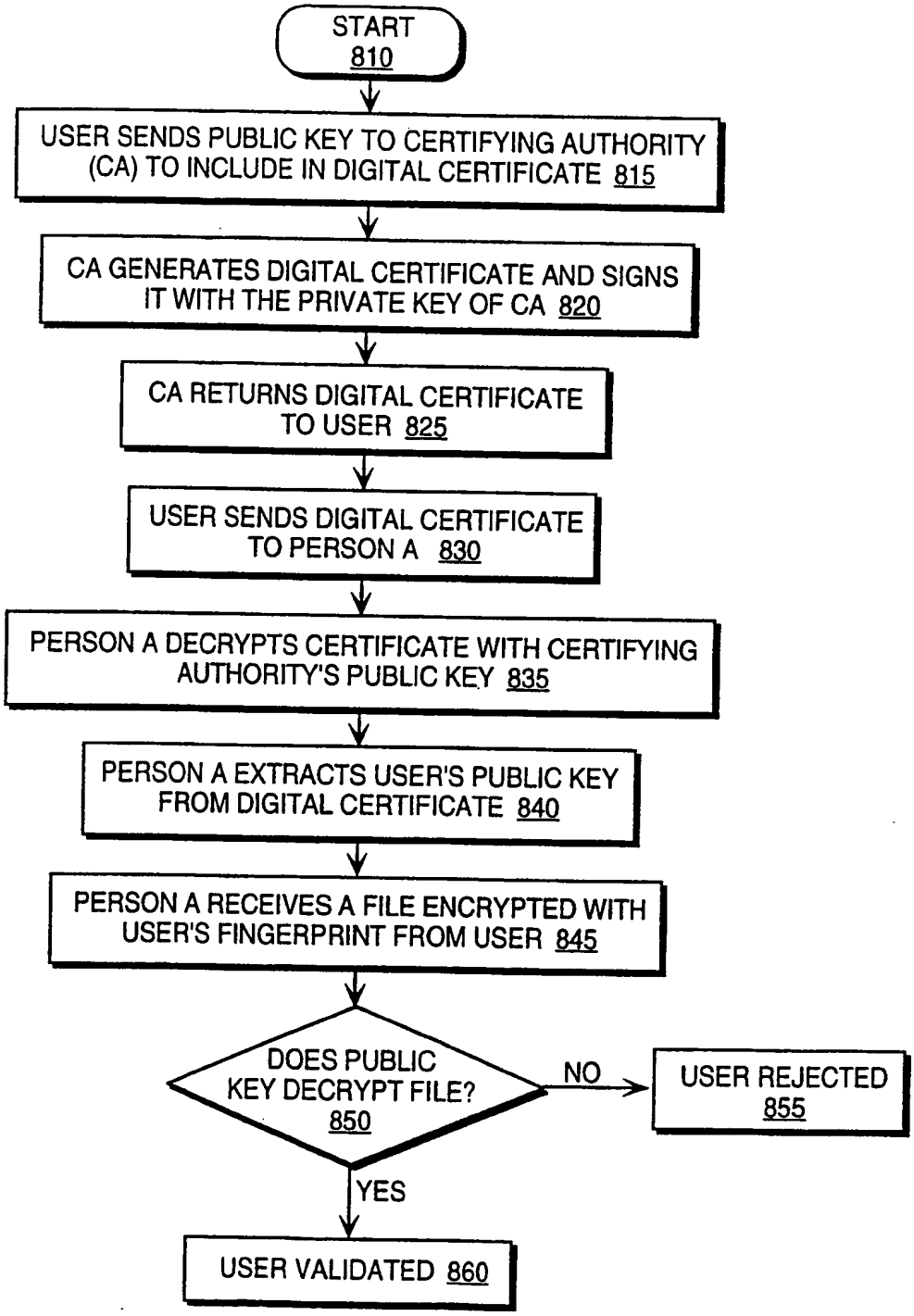

START 810
USER SENDS PUBLIC KEY TO CERTIFYING AUTHORITY (CA) TO INCLUDE IN DIGITAL CERTIFICATE 815
CA GENERATES DIGITAL CERTIFICATE AND SIGNS IT WITH THE PRIVATE KEY OF CA 820
CA RETURNS DIGITAL CERTIFICATE TO USER 825
USER SENDS DIGITAL CERTIFICATE TO PERSON A 830
PERSON A DECRYPTS CERTIFICATE WITH CERTIFYING AUTHORITY'S PUBLIC KEY 835
PERSON A EXTRACTS USER'S PUBLIC KEY FROM DIGITAL CERTIFICATE 840
PERSON A RECEIVES A FILE ENCRYPTED WITH USER'S FINGERPRINT FROM USER 845
DOES PUBLIC KEY DECRYPT FILE? 850
NO
USER REJECTED 855
YES
USER VALIDATED 860

FIG. 8

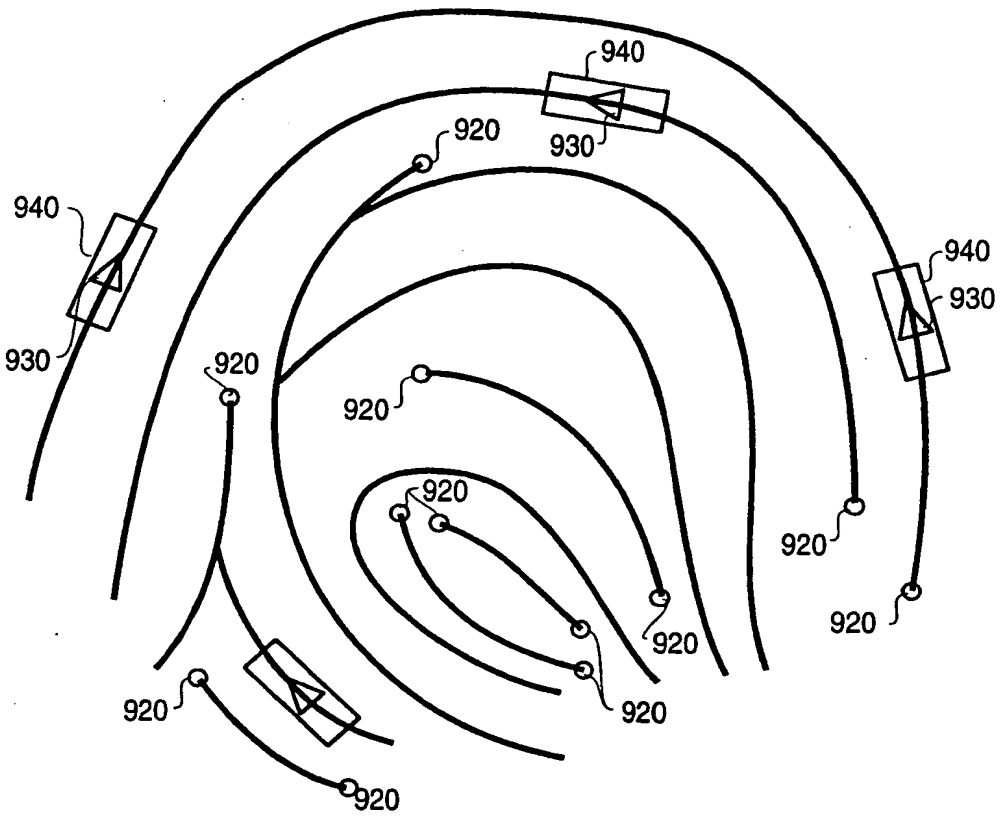


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/23327

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04L 9/32, G06K 9/00
US CL : 380/23, 382/181,199, 203, 206, 209
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 382/181,199, 203, 206, 209

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Your Information Technology Source, Biometric Digest

www.fingerprint.com

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,493,621 A (MATSUMURA) 20 February 1996	1-22
X, P --- Y	US 5,712,912 A (TOMKO ET AL.) 27 January 1998, col. 4, line 1-17; col. 11, line 10-29; col. 10, line 62-67 to col. 11, line 1-8; col. 12, line 34-53; col. 16, line 5-19; col. 39, line 20-43	1-4, 8-11, 13 and 15 --- 12, 14
Y, P	US 5,799,098 A (ORT ET AL.) 25 August 1998, col. 28, line 26-30	12
Y	US 5,841,865 A (SUDIA) 11 April 1997, col.14, line 34-35; col. 51, line 44-59	21,22
Y, P	US 5,768,382 A (SCHNEIER ET AL) 16 June 1998, col. 15, line 37-48; col. 16, line 20-25; col. 17, line 50-62	21,22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 20 JANUARY 1999	Date of mailing of the international search report 22 APR 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer TODD M. JACK Joni Hill Telephone No. (703) 305-1027

Form PCT/ISA/210 (second sheet)(July 1992)*